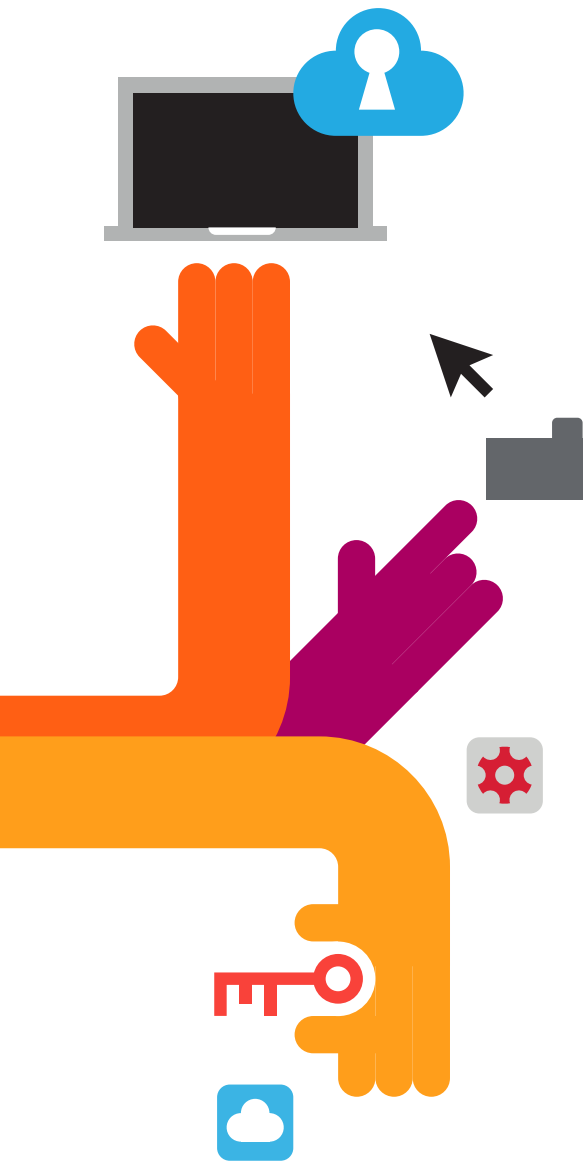




Unlock opportunity with a new security approach

Gain the flexibility and control you need to
advance innovation, manage risk, and enable
new ways of working





Contents

The world of work is changing	3
Simplifying security in a cloud-first world.....	5
The Citrix secure digital workspace unifies everything	7
A people-centric security approach	9
Trusted framework for securing the digital workspace.....	10
Essential elements of a secure digital perimeter	11

The world of work is changing

It used to be that work was a place. Not anymore. Today, it's an increasingly dynamic activity that people expect to be as adaptable as they are. People are trading in the cubicles and desktops for virtual meetings and mobile devices.

To power this new way of working and support strategic business objectives, organizations have embraced user-friendly SaaS and cloud-based services. But managing a proliferation of apps and data scattered across clouds and data centers is unwieldy, increases your security risks, and puts a strain on productivity.

Traditional security perimeters built around the corporate data center worked as long as apps, data, and employees were all behind the corporate firewall. But as work extends beyond the firewall to include virtual, web, and SaaS apps, the old way of layering fragmented point solutions is no longer enough to keep you ahead of ever-evolving threats.

A new security framework is needed to secure your apps and data across the clouds, devices, and networks where business is happening and people are collaborating.



3

Number of devices employees use daily for work activities.¹



36

Number of cloud services the average employee actively uses at work²

83%

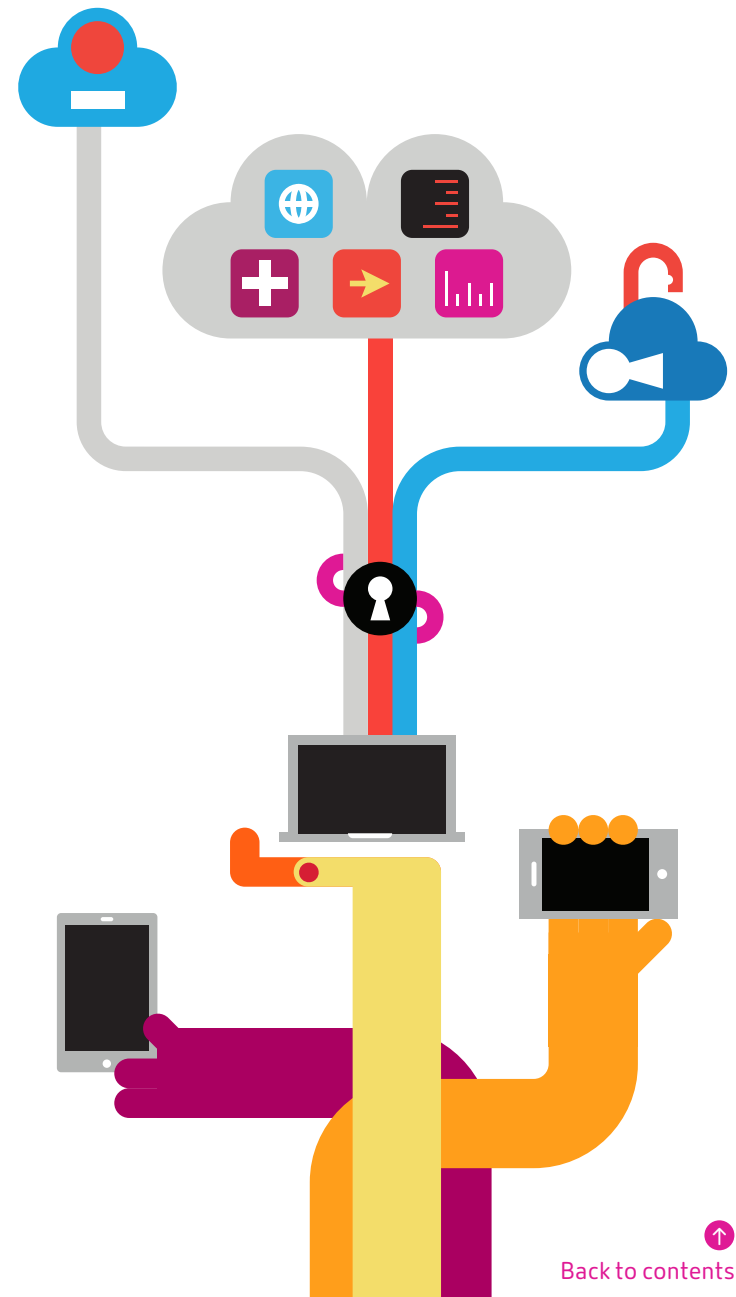
of organizations say complexity of their organizational structures and IT infrastructure puts them at even greater risk for security breaches.³

Simplifying security in a cloud-first world

A confident security strategy can help you see opportunity — not vulnerability — in a rapidly expanding array of devices, apps, services, and cloud infrastructure. A holistic approach gives you the flexibility and control to balance security risk with the need to advance innovation, growth, and new ways of working.

A secure digital workspace is a contextual, integrated way to deliver and manage the apps, desktops, data, and devices your users need to be productive. It can fully aggregate all apps and data — both on premises and cloud — to deliver the right experience to the right user at the right time.

Protected by a secure digital perimeter that surrounds users wherever they are, a digital workspace gives IT, security, and networking teams simplified control and proven security across today's hybrid, multi-cloud, and SaaS environments.



74%

of enterprises agree — a new IT security framework is needed to improve security posture and reduce risk.³

The Citrix secure digital workspace unifies everything

Apps and desktops

Secure, remote access to web, SaaS, and virtual applications and desktops from any device, over any network.

Unified endpoint management

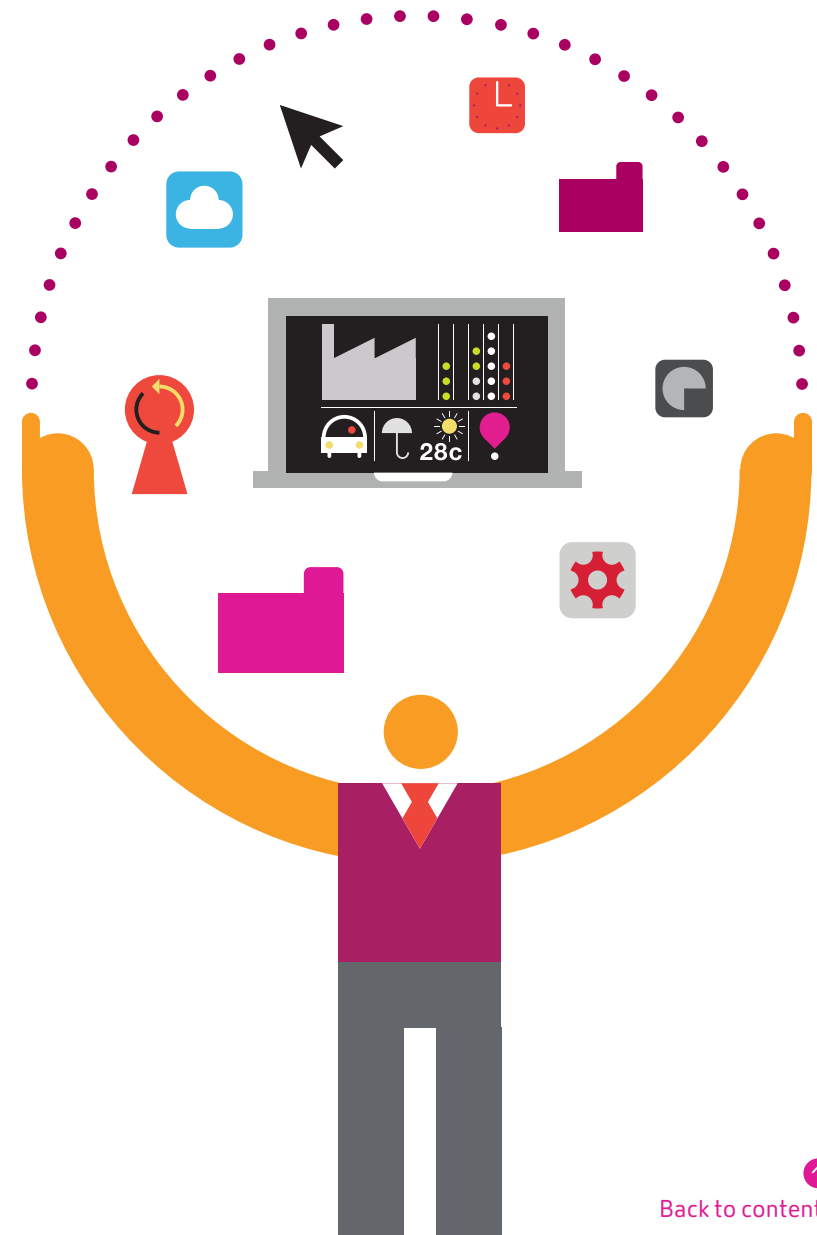
Full access to mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), secure network gateway, and enterprise-grade mobile productivity apps.

Data

Access, sync, and securely share files from any device, with full control for IT.

Networking

A secure digital perimeter provides reliability, performance, analytics, and security for apps deployed in the data center, cloud, or delivered as SaaS.





**Innovation drives the future.
Citrix is leading the charge
in security innovation with
their revolutionary approach to
protecting mission-critical data.**

— Jeff Kater, Director of IT, KDFA

A people-centric security approach

In the same way a digital workspace provides access to apps and data from anywhere, the network perimeter must dynamically expand beyond the data center to protect information and users wherever they are. Our modern, people-centric approach to reliability, performance, and security for apps deployed in the data center, cloud, or delivered as SaaS. It gives you:

Simplified control

- People-centric policies based on identity
- Centralized management and distributed policy enforcement across various control points — apps, content, devices, networks — in hybrid and multi-cloud environments
- Protection of application infrastructure by hiding or minimizing attack surfaces
- Easily enabling compliance to regulatory standards

360-degree visibility

- Full visibility across your entire infrastructure
- Recording and aggregating logs and transaction flows between users, apps, devices, content, and networks

Intelligent analytics

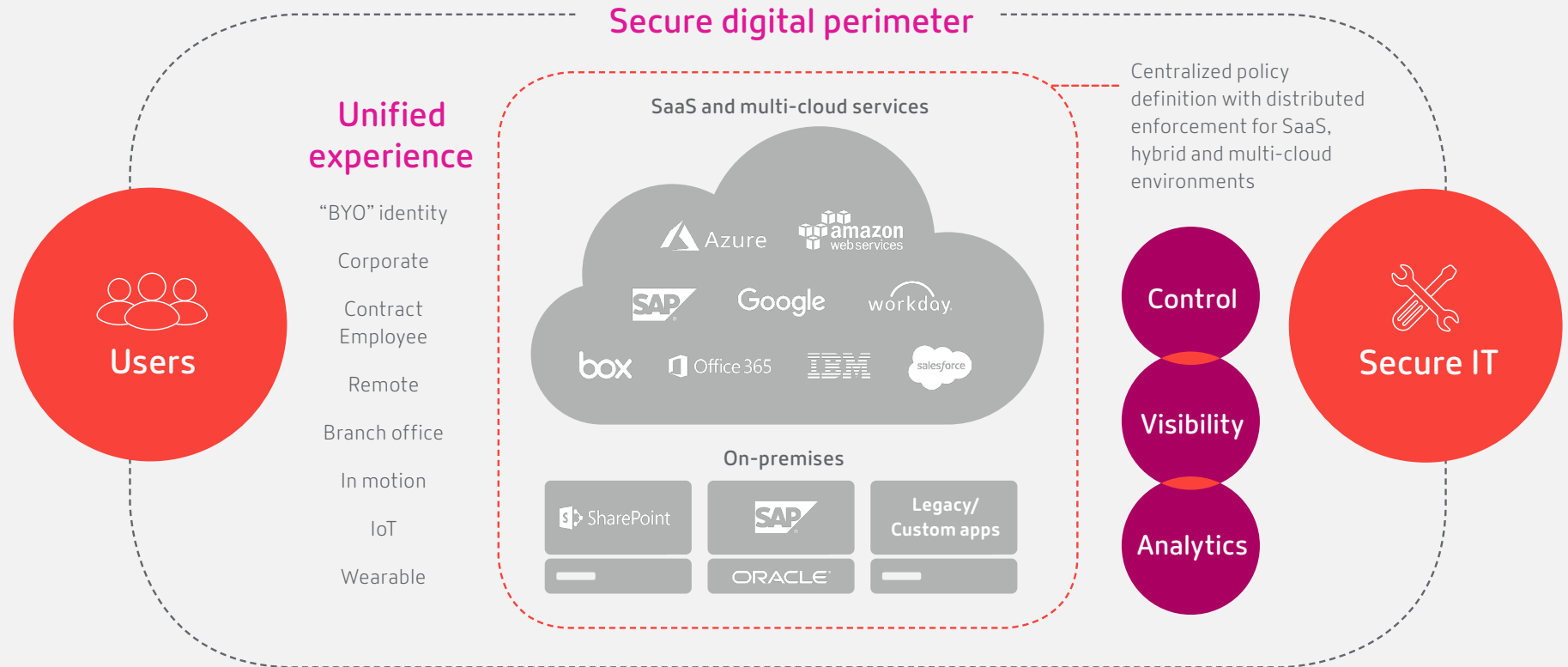
- Providing insights by analyzing patterns for cyber threats, app and network performance changes, infrastructure usage, and user behavior anomalies
- Triggering of automated policy-based actions for access control, threat management, IP protection, and high availability

“We didn’t want people tethered to their desks. With Citrix, we’ve given people the freedom to sit where they want, to collaborate and to work in an environment that works for them.”

— Jeff Miller, Head of IT Services, Registers of Scotland

Trusted framework for securing the digital workspace

- Deliver an on-demand people-centric security perimeter
- Minimize and hide attack surfaces
- Get full visibility across SaaS, hybrid, and multi-cloud environments
- Automate contextual actions and policies based on triggers
- Share threat intelligence across services to prevent malicious actions and behaviors



Essential elements of a secure digital perimeter

Contextual and secure access

User identity is core to a people-centric approach. Deliver a simple, personalized experience to each user based on context and preferences. Set contextual policies to automatically adapt to changing conditions—grant or revoke access based on the user, location, device, or suspicious activity. Provide single sign-on (SSO) across web, SaaS, and virtual apps to simplify IT management and provide a better user experience.

Mobile and device security

Enable your mobile workforce and secure corporate and BYO devices by seamlessly applying device and app control policies. Provide end-to-end encryption to secure data as it moves between the endpoint, network, and company resources. Leverage sophisticated container technology to secure apps and data on the device with a high-security encrypted vault for key storage.

Reduce exposure to insider and outsider threats

Because you have visibility across endpoints, the network path, web traffic, data repositories, and web, virtual, and SaaS applications, it's easier to detect malware. Isolate high-target apps to protect them against attacks. Inspect browsing activity and redirect suspicious site access to a safer, sand-boxed location to prevent any malicious activity or harmful data from entering the perimeter. Using policies, you can centrally control and manage blocked sites.

Secure collaboration with data security and intellectual property (IP) protection

Secure your most sensitive business data, whether it's in use, in motion, or at rest in the data center or the cloud. Exchange and collaborate on documents easily and securely while ensuring industry-standard AES 256 encryption of all meta-data and content. Integrate with data loss provider (DLP) solutions for visibility and control over the sharing of sensitive data.

Governance, risk, and compliance

Easily demonstrate compliance with visibility across your entire infrastructure. Better enforce compliance and governance aspects such as information rights management (IRM) and data loss prevention (DLP) by integrating users' roles and responsibilities directly into how they use and interact with apps and data. This makes it easier to detect and prevent external or internal malicious attempts to steal sensitive data.

Business continuity

Create a more coordinated approach to application security by gathering input from the network and from web, virtual, and SaaS apps. Ensure the availability and performance of apps and services to users at all times through always-on connectivity, even during server or network outages, and protection against attacks that aim to disrupt business operations.



[Back to contents](#)



The freedom to innovate

Let Citrix help you enable all the ways your employees want and need to work while remaining confident that your data, apps, and network are secure. Engineered to empower IT with control and users with flexibility, our comprehensive security approach gives you the freedom to adopt new innovations that will advance your business priorities and support new ways of working with confidence.



Learn more at Citrix.com/secure.

Sources:

1. "7 Enterprise Mobility Statistics You Should Know," 2015, Citrix.com
2. 12 Must-Know Statistics on Cloud Usage in the Enterprise," 2016, Skyhigh
3. "The Need for a New IT Security Architecture," Ponemon Institute, sponsored by Citrix, 2017



[Back to contents](#)